UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/553,306	10/14/2005	Yuliang Zheng	46872/319100	1967

44231 7590 09/11/2007

KILPATRICK STOCKTON LLP - 46872
J. STEVEN GARDNER
1001 WEST FOURTH STREET
WINSTON-SALEM, NC 27101

EXAMINER	
HUSSAIN, IMAD	

ART UNIT	PAPER NUMBER
2109	

MAIL DATE	DELIVERY MODE
09/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/553,306	ZHENG ET AL.	
	Examiner	Art Unit	
	Imad Hussain	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *06/26/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been filed in parent Application No. PCT/US03/016817, filed on 30 May 2003.

Claim Objections

2. Applicant is advised that should claim 3 be found allowable, claim 4 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 2, 5-8, and 10-17 are rejected under 35 U.S.C. 102(e) as being anticipated by John B. Beavers (US PGPub 2003/0221123 A1, hereafter Beavers).

Regarding claim 1, Beavers teaches a network security system, comprising:

a static policy data store [*set of rules*, claim 1];

a dynamic policy data store [*decision table*, claim 1; *dynamic threat table*, paragraph 54; *dynamic tracking table*, paragraph 98];

an authorization enforcement facility (AEF) [*alert processing system,* claim 12, figure 5 (63)] in communication with said static policy data store [(27)] and said dynamic policy data store [(31)] and operable to perform a risk-aware analysis of a connection [*matching* and *declaring an incident*, claim 1].

Regarding claim 2, Beavers teaches that the static policy data store comprises at least one of a constraint, a role, a node-role assignment, a threshold value [*a threshold value from a user-editable table*, claim 5], a node value, a service value, and an action value.

Regarding claim 5, Beavers teaches that the dynamic policy data store comprises a threat level table [*table with threat characterizations*, claim 5].

Regarding claim 6, Beavers teaches that the system is further operable to generate a response to said connection [*an action as a mitigating response can be taken*, paragraph 39].

Regarding claim 7, Beavers teaches that the response comprises at least one of blocking the source of said connection from connecting to an intended destination [*an action as a mitigating response can be taken. An example would be to shut down a web server that is suspected of being compromised,* paragraph 39], altering said intended destination of said connection [after an alert, *the information is trashed or diverted at line 25*, paragraph 33], and auditing said connection [paragraph 3].

Regarding claim 8, the claim recites the same limitations as claim 7 and is rejected by the same rationale.

Regarding claim 10, Beavers teaches that the system comprises a router, a gateway, a hardware appliance [*firewall, IDS, router,* etc., paragraphs 105-114], or a web server [claim 15].

Regarding claim 11, Beavers teaches that the system further comprises a firewall [paragraph 109] in communication with said AEF [*alert processing system*].

Regarding claim 12, Beavers teaches that the system further comprises an intrusion detection system [*IDS,* paragraph 113] in communication with said AEF [*alert processing system*].

Regarding claim 13, Beavers teaches a method comprising:

receiving a static policy data attribute from a static policy data store [*set of rules,* claim 1; Fig 5 (27)];

receiving a connection request directed to a node [paragraphs 2-3]

receiving a dynamic policy data attribute from a dynamic policy data store [*decision table,* claim 1; Fig 5 (31)];

determining whether said connection request is anomalous based at least in part on said static policy data attribute [*set of rules,* claim 1] and at least in part on said dynamic policy data attribute [*decision table,* claim 1].

Regarding claim 14, the claim comprises the limitations of claims 13 and 6 and is rejected by the same rationale.

Regarding claim 15, the claim comprises the limitations of claims 14 and 7 and is rejected by the same rationale.

Regarding claim 16, Beavers teaches updating said dynamic policy data attribute in said dynamic policy data store based on a result of said determining [*incident tracking rules can be automatically updated based on one or more further alert indications*, paragraph 15].

Regarding claim 17, Beavers teaches increasing a threat level if the connection request is determined to be anomalous [*If the non-condition alert passes the threshold, this*

information can be added to existing incident tickets, and the incident ticket tracking rules can be updated with this information, paragraph 97; the rules referencing *the table with the time, the status, the threat level, and an incident description*, paragraph 40].

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beaver in further view of Frederick M. Avolio (*Best Practices in Network Security*, hereafter Avolio).

Regarding claim 3, Beaver states that *the threshold value can be a level of severity* [paragraph 13] and that severity is defined *on a scale of 1-5 (1 being the highest threat)* [paragraph 36]. Beaver does not explicitly disclose that the threshold value is inversely proportional to the node value.

However, Avolio teaches (page 2 column 3) that the severity of a threat is based upon the value of the object being secured. It would have been obvious at the time that the invention was made to combine these teachings such that the higher the value of an object, the lower the threshold value is set, i.e., setting the threshold value inversely proportional to the node value.

Beaver and Avolio are analogous subject matter in the same field of endeavor as both cover network security. One of ordinary skill in the art would have been motivated to combine the threshold-severity relation taught by Beavor with the severity-value relation taught by Avolio because doing so allows for a basis by which to set the severity, and hence the threshold, level for object. Therefore, the claimed invention as a whole would have been "*prima facie* obvious" to one of ordinary skill at the time the invention was made.

Regarding claim 4, the claim recites the same limitations as claim 3 and is rejected by the same rationale.

7. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Beaver as exemplified by Tom Chmielarski (*Intrusion Detection FAQ: Reconnaissance Techniques using Spoofed IP Addresses,* hereafter Chmielarski).

Regarding claim 9, Beaver teaches that a countermeasure may be taken and that the countermeasure may comprise a passive countermeasure [*an action as a mitigating response can be taken. An example would be to shut down a web server that is suspected of being compromised*, paragraph 39].

Beaver does not explicitly disclose that the countermeasure comprises an active countermeasure.

However, Chmielarski teaches both active and passive countermeasures [whole document] in the context of intrusion detection systems.

Beaver and Chmielarski are analogous subject matter in the same field of endeavor as both cover intrusion detection systems. One of ordinary skill in the art would have been motivated to combine the general countermeasures taught by Beaver with the active countermeasures taught by Chmielarski because doing so allows for the system to analyze and understand methods used by attackers and better protect against further attacks. Therefore, the claimed invention as a whole would have been "*prima facie* obvious" to one of ordinary skill at the time the invention was made.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Bernhard; Thomas et al. *System, method and computer program product for automatic response to computer system misuse using active response modules* US 6275942 B1 (Describes a system to monitor and respond to anomalies.)

b. Lermuzeaux; Jean-Marc et al. *Facility for detecting intruders and suspect callers in a computer installation and a security system including such a facility* US 5621889 A (Describes a system to monitor and respond to anomalies.)

c. Campbell; Wayne A. et al. *Method and system for detecting intrusion into and misuse of a data processing system* US 6839850 B1 (Describes a system to monitor and respond to anomalies.)

d. Judge; Paul et al. *Systems and methods for adaptive message interrogation through multiple queues* US 7089590 B2 (Describes a system to monitor and respond to anomalies.)

e. Hu; Wei-Ming. *Network request distribution based on static rules and dynamic performance data* US 6173322 B1 (Describes a system to monitor and redirect requests.)

f. Nessett; Danny M. et al. *Multilayer firewall system* US 5968176 A (Describes a network security system including packet filtering and inspection.)

g. Thomas; R.K. et al. *Task-based Authorization Controls (TBAC)*. IFIP (Describes task and role-based authorization methods.)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Imad Hussain whose telephone number is 571-270-3628. The examiner can normally be reached on Monday through Thursday from 0730 to 1700.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Beatriz Prieto can be reached on 571-272-3902. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Imad Hussain

Beatriz Prieto

BEATRIZ PRIETO
SUPERVISORY PATENT EXAMINER